



OAUTH UND AUTORISIERUNGSMODULE IN SERVICE ORIENTED ARCHITECTURE

PRODUKT

- Aktivitäts- und zeitmanagementorientiertes soziales Netzwerk
- eine Alternative zum klassischen Ticketsystem (Jira)
- Auf Privatpersonen orientiert

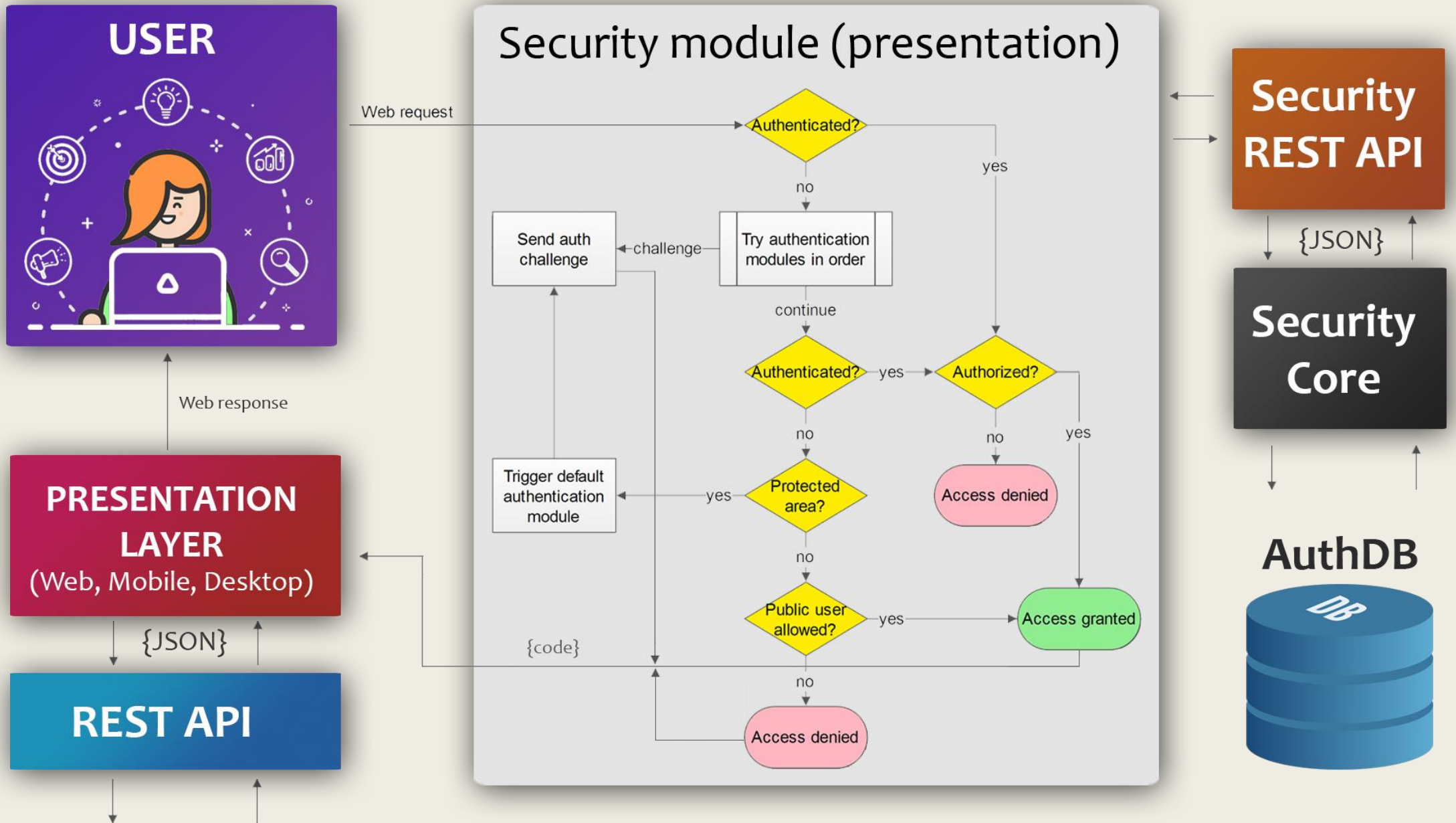


Rechtliche Anforderungen

- TMG § 5 Allgemeine Informationspflichten
- TMG § 13 Pflichten des Diensteanbieters
- UrhG § 22

Architekturkonzept

- Umstieg von monolithic architecture to SOA
- Auslagern von Autorisierungslogik
- Verwendung von Frameworks
- Hierarchische Berechtigungssystem



OAuth v2.0

- OAuth 2 = Autorisierungsframework
- Eingeschränkter Zugriff auf Benutzerkonten in HTTP-Diensten
- OAuth (Open Authorization) ist ein offenes Protokoll
- Unterstützt Web-, sowie Desktop- bzw. Mobile Applikationen.

Systemhierarchie und Konzept:

- **Kontoinhaber:** Der Benutzer autorisiert sein Konto. Der Zugriff einen Dienst auf dem Benutzerkonto ist beschränkt (lesende- oder schreibende Zugriff).
- **Ressourcenserver und Autorisierungsserver: API** Der Ressourcenserver speichert die geschützten Daten von Benutzerkonten und der Autorisierungsserver verifiziert die Authentizität der vom Benutzer bereitgestellten Informationen und erstellt dann Autorisierungstoken für die Anwendung, über die die Anwendung auf Benutzerdaten realisiert wird. Aus Sicht des Anwendungsentwicklers führt die Service-API sowohl die Ressourcenserverrolle als auch die Autorisierungsserverrolle aus.
- **Client: externer Service**
Applikation bzw. Dienst, die auf das Benutzerkonto zugreifen, muss vor dem Zugriff vom Benutzer autorisiert werden und die Autorisierung muss von der API kontrolliert werden.

Abstraktes Konzept

